UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,472	01/26/2001	Jean Louis Calvignac	RAL920000119US1	6208

25299 7590 06/13/2006

IBM CORPORATION
PO BOX 12195
DEPT YXSA, BLDG 002
RESEARCH TRIANGLE PARK, NC 27709

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 06/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/771,472	CALVIGNAC ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 February 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: 28 February 2006 with acknowledgement of an original application filed 26 January 2001.

2. Claims 1-20 are currently pending in this application. Claim 6 has been amended, claims 9-20 are new. Claims 1, 16, and 19 are independent claims.

Response to Arguments

3. Applicant's arguments filed 28 February 2006 have been fully considered but they are not persuasive.

In response to applicant's argument on page 8, "However, Applicants submit that GREENE does not disclose, or even suggest, combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle. Nor has the Examiner identified any language in GREENE which discloses or suggest this feature". The Examiner disagrees with argument presented. GREENE teaches that combination logic outputting data in a single hardware cycle see col. 4, line 58 through col. 5, line 13. In GREENE the single hardware cycle has the same meaning as a cycle of an encryption circuit.

In response to applicant's argument beginning on page 8, Furthermore, while the Examiner has interpreted a single hardware cycle as an encryption circuit", the Examiner has failed to appreciate the face that paragraph [0007] of the instant published application defines a single hardware cycle as a cycle that may take several clock cycles and one wherein the crypto-function is implemented in the combination logic without intermediate registers that require loading and setting time before contents of the intermediate registers can be read". The

Examiner disagrees with argument presented. GREENE shows that the encryption circuit can take several clock cycles and the loading and setting time can be done via the combinational logic, see col. 5, line 6-12, that explains the encryption circuit can have a multiple clock cycles "T"; and see col. 6, lines 50-58 that summarizes the action of the scheduler and how it operates to pipeline the encryption operation, which is interpreted to be equivalent to "combination logic without intermediate registers".

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 9, 11, 13, and 17-20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 9, 11, and 17-20, are objected to because the claims contain the following limitation "clock cycle" which is indefinite because the amount of time is not constant.

Claim 13 is objected to because "depend solely on their inputs" is indefinite and fails to further limit the invention.

6. To expedite a complete examination of the instant application the claims rejected under 35 U.S.C. § 112 above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

8. **Claims 1-20** are rejected under 35 U.S.C. 102(e) as being anticipated by Greene U.S. Patent No. 6,870,929 (hereinafter '929).

As to independent claim 1, "A hardware implementation of a crypto-function comprising: a first register storing data to be encrypted or decrypted;" is taught in '929 col. 4, lines 6-31;

"a second register for receiving data which has been encrypted or decrypted" is shown in '929 col. 5, lines 1-5;

"and combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle" is disclosed in '929 col. 5, lines 6-12 (Note "combinational logic performing computation iteration of the crypto-function" is interpreted to have the same meaning as 'a number of cipher stages", also note "a single hardware cycle" is interpreted to have the same meaning as 'an encryption circuit').

As to dependent claim 2, "wherein the crypto-function is a block cipher algorithm" is taught in '929 col. 6, lines 58-67.

As to dependent claim 3, "wherein the crypto-function is the Data Encryption Standard (DES) algorithm" is shown in '929 col. 6, lines 58-67.

As to dependent claim 4, "wherein the crypto-function is the CHAIN algorithm" is disclosed in ''929 col. 6, lines 58-67.

As to dependent claim 5, "wherein the combinational logic performs an invertible key-dependent round function iterated a predetermined number of times" is taught in '929 col. 7, lines 7-21 and col. 7, line 62 through col. 8, line 4.

As to dependent claim 6, "wherein the combinational logic performs mixing, permutation and key-dependent substitution in each round" is shown in '929 col. 7, lines 7-21 and col. 8, lines 6-32.

As to dependent claim 7, "wherein the combinational logic enciphers a block by performing an initial permutation of a block to be enciphered and then a complex key-dependent computation followed by a permutation which is an inverse of the initial permutation" is disclosed in '929 col. 7, lines 51-67.

As to dependent claim 8, "wherein the combinational logic deciphers a block by performing deciphering using the same key as used to encipher the block in a process that is an inverse of the enciphering process" is taught in '929 col. 10, lines 8-17.

As to dependent claim 9, "wherein the one hardware cycle is approximately ten clock cycles" is shown in '929 col. 5, lines 7-12.

As to dependent claim 10, "wherein the hardware implementation of the crypto-function uses only the combinational logic without having to store intermediate results in registers" is disclosed in ''929 col. 4, lines 58-67.

As to dependent claim 11, wherein the hardware implementation the crypt-function computes an iterated round function in one clock cycle" is taught in '929 col. 5, lines 7-12.

As to dependent claim 12, "wherein the combination logic utilizes a Data Encryption Standard (DES) algorithm that is implemented in the combination logic" is shown in '929 col. 6, lines 58-67.

As to dependent claim 13, "wherein the combination logic utilizes logic functions whose outputs depend solely on their inputs" is disclosed in '929 col. 5, lines 12-23.

As to dependent claim 14, "wherein the combination logic utilizes logic circuits without memory, whereby no registers are used to store intermediate results or iterations of encipher or deciphering computations" is taught in '929 col. 4, lines 29-67.

As to dependent claim 15, "wherein the crypt-function is implemented in the combinational logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read" is shown in '929 col. 4, lines 58-67.

As to independent claim 16, "A hardware implementation of a crypto-function comprising: a first register that stores data to be encrypted or decrypted; a second register that receives data which has been encrypted or decrypted; and combinational logic that performs computation iteration of the crypto-function on data store in the first register" is taught in '929 col. 4, lines 6-31;

"and outputting data to said second register" is shown in '929 col. 5, lines 1-5;

"in a single hardware cycle, wherein the crypt-function" is disclosed in '929 col. 4, 58-67;

"is implanted in the combination logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read" is taught in '929 col. 5, lines 6-12 (Note "combinational logic performing computation iteration of the crypto-function" is interpreted to have the same meaning as 'a number of cipher stages", also note "a single hardware cycle" is interpreted to have the same meaning as 'an encryption circuit').

As to dependent claim 17, "wherein the single hardware cycle is approximately ten clock cycles" is disclosed in ''929 col. 4, lines 58-67.

As to dependent claim 18, wherein the hardware implementation of the crypto-function computes and iterated round in just one clock cycle" is disclosed in ''929 col. 4, lines 58-67.

As to independent claim 19, "A hardware implementation of a crypto-function comprising: a first register that stores data to be encrypted or decrypted; a second register that receives data which has been encrypted or decrypted; and combination logic that performs computation iteration of the crypto-function on data stored in the first register" is taught in '929 col. 4, lines 6-31;

"and outputting data to said second register" is shown in '929 col. 5, lines 1-5;

"in a single hardware cycle" is disclosed in '929 col. 4, 58-67;

"wherein the single hardware cycle comprises several clock cycles" is taught in '929 col. 5, lines 8-12.

As to dependent claim 20, "wherein the cypt-function is implemented in the combination logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read" is shown in '929 col. 4, lines 58-67.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 8:00 am to 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ECT

Ellen Tran
Patent Examiner
Technology Center 2134
7 June 2006